

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW JERSEY**

---

INDUSTRIENS PENSIONSFORSIKRING  
A/S, Individually and on behalf of all others  
similarly situated,

Plaintiff,

vs.

BECTON, DICKINSON AND COMPANY,  
and THOMAS E. POLEN,

Defendants.

---

Civil Action No.: 2:20-cv-02155-SRC-  
CLW

**STIPULATION AND ORDER  
REGARDING  
ELECTRONICALLY STORED  
INFORMATION**

This Agreement and Order will govern how the parties manage electronic discovery in the above-captioned action.

## **I. PRESERVATION**

Consistent with the parties' obligations under Rule 26(f) of the Federal Rules of Civil Procedure, the parties will meet and confer regarding the scope of preservation. The parties will disclose categories and sources of information relating to the subject matter of this litigation that they have reason to believe have not been preserved or should not be preserved and will explain with specificity the reasons to support such a belief.

## **II. COLLECTION AND SEARCH GUIDELINES**

The parties shall meet and confer in an effort to conduct discovery in an efficient and effective manner. Specifically, and as discussed further below, within a reasonable period of time after the Rule 26(f) conference, the parties will meet and confer regarding any proposed limitations on the scope of discovery, including custodians and their data sources, non-custodial and other data sources, date ranges, file types, and any proposed method to cull documents for review (e.g., whether the producing party intends to apply search terms, analytics, including de-duplication, email threading, or technology-assisted review). The parties will disclose all such proposed measures for identifying and culling documents for review, and will attempt in good faith to come to an agreement on any culling and search methods used to identify responsive information. The parties intend, and will confer in good faith during their initial discussions regarding the scope of discovery, to agree upon a date by which they will substantially complete document productions. The parties will not seek Court intervention without first attempting to resolve any disagreements in good faith, based upon all reasonably available information.

**A. Identification of Custodians and Non-Custodial Data Sources.** The parties agree to meet and confer regarding the appropriate custodians and their data sources, as well as non-

custodial and other data sources to be collected and searched for this litigation. Within a reasonable period of time after the Rule 26(f) conference, the parties will provide a list of the custodians and their data sources, as well as non-custodial and other data sources whose data will be collected and searched for potentially responsive documents—including but not limited to any mobile devices or tablets, messaging or chat applications or programs, and any collaborative tools or platforms, as well as any relevant electronic systems and storage locations—including but not limited to back-up tapes and cloud storage. The parties will also disclose and describe any document retention policies or practices (e.g., retention schedules or policies, auto-delete functions, routine purging, mailbox size limits), archiving systems with size limitations on the number of emails searched or exported (e.g., Mimecast, Barracuda), or other policies or practices, likely to impact the existence, accessibility, or ability to collect responsive documents or electronically stored information (e.g., bring your own device policies or other policies applicable to laptops, mobile devices or tablets distributed to employees). The parties will also identify and describe custodial data sources, and non-custodial data sources reasonably likely to contain information relevant to the subject matter of this litigation that they assert should not be searched or are not reasonably accessible and will explain the reasons for such assertions. Additionally, the parties will disclose third-party sources, if any, reasonably likely to contain discoverable information. The parties retain the right, upon reviewing the opposing party's production of documents, and conducting other investigation and discovery, to request that files from additional custodial, non-custodial, cloud-based, or other sources be searched, and will meet and confer regarding any such request.

**B. Custodians.** In connection with the parties' meet and confer efforts, the parties shall produce organizational charts to the extent any such charts exist, for all business units in which custodians identified pursuant to paragraph II.A worked at relevant times, and, for each

proposed custodian, indicate the person's job title(s), the time period(s) when they held such position(s), and a brief description of their responsibilities in each position held.

**C. Culling.** Parties shall de-duplicate documents prior to review and production using the methods described in paragraph II.D. below. The parties may not use email threading to cull the dataset prior to review. To the extent a party intends to use any other filters or culling mechanisms (e.g., date ranges, search terms, or technology assisted review) to reduce the volume of data to review for responsiveness, it shall disclose all such methodologies to the receiving party and the parties agree to meet and confer regarding such measures.

**D. De-Duplication.** Prior to review, each party may remove exact duplicate documents based on MD5 or SHA-1 hash values, in a manner that does not break-up document families. Attachments should not be eliminated as duplicates for purposes of de-duplication, unless the parent email and all attachments are also duplicates. The parties agree that an email that includes content in the BCC or other blind copy field shall also not be treated as a duplicate of an email that does not include content in those fields, even if all remaining content in the email is identical. Removal of near-duplicate documents is also not acceptable, and lesser included emails are not considered a duplicate of a more inclusive email thread, and may not be removed as a means of culling the data set for review. Further, while a party may utilize near-duplication and email threading tools to conduct its review, neither of these tools may be employed for purposes of producing ESI in response to a discovery request in this Action. De-duplication will be done across the entire collection (global de-duplication) and the CUSTODIAN-ALL field will list each custodian, separated by a semicolon, who was a source of that document. Should the CUSTODIAN-ALL metadata fields produced become outdated due to rolling productions, an overlay file providing all the custodians and file paths for the affected documents will be produced

with each production that rendered those fields outdated.

**E. Discovery Not Required.** The parties need not produce the following ESI:

1. Standard system file extensions, including but not limited to BIN, CAB, CHK, CLASS, COD, COM, DLL, DRV, INF, INI, JAVA, LIB, and SYS.
2. Files identified by hash value when compared to the National Software Reference Library reference data set (RDS Hash), a sub-project of the National Institute of Standards and Technology (NIST), of known traceable system and application files. This process is commonly referred to as “De-NISTing.”
3. Data that is fragmented, in unallocated space, or only accessible by forensics;
4. Data stored in random access memory (RAM), cache memory, or in temporary or cache files, including internet history, web browser cache, and cookie files; and
5. Data stored on photocopiers, scanners, and fax machines;

### **III. SEARCH METHODOLOGY**

**A. Transparency.** The parties will undertake best efforts to reach agreement regarding an appropriate search methodology for identifying responsive documents. In connection with these efforts, the parties agree to: (i) disclose the search methodology they intend to use to identify responsive documents; (ii) be transparent regarding the inputs, restrictions, and other parameters applicable to such methodology; (iii) disclose any intended changes to a previously disclosed search methodology prior to effectuating such change; and (iv) disclose methods proposed to validate the party’s search methodology.

**B. Easily Targeted Responsive Documents.** Documents and categories of documents that are relevant to this action and responsive to a party’s document requests, and that

are regularly maintained in a known location, or in a location that is knowable upon reasonable inquiry of those with knowledge about a party's document management systems, shall be collected without the use of search terms or other agreed-upon advanced search methodology (e.g., analytics, predictive coding, technology-assisted review). The producing party will indicate which categories of documents will be produced with and without the use of search terms or other advanced search methodology. Where potentially responsive ESI shall be identified through the use of search terms or other agreed-upon advanced search methodology, the parties agree to follow the process identified below and the parties shall meet and confer regarding any proposed deviation.

**C. Search Terms.** Where the parties agree that potentially responsive ESI shall be identified through the use of search terms, the parties shall meet and confer within a reasonable time after the Rule 26(f) conference, regarding the process to be used. The producing party shall provide a list of proposed search terms, which shall contain all search terms that it believes would lead to the identification of relevant documents. To the extent reasonably possible, search terms will be crafted with input from the custodians in order to identify appropriate nomenclature, code words, etc. The parties shall meet and confer regarding the proposed search terms within a reasonable period of time after the requesting party's receipt of the search terms to agree on a set of search terms. If disputes still exist at the end of the meet-and-confer process, the parties will submit such disputes to the Court pursuant to the Court's practices and procedures for raising discovery disputes.

**D. Technology-Assisted Review.** No party shall use predictive coding/technology-assisted review for the purpose of culling the documents to be reviewed, or identifying responsive documents to be produced, without notifying the opposing party prior to its use with ample time to meet and confer in good faith regarding a mutually agreeable protocol for the use of such

technologies.

**E. Validation.** The parties will meet and confer regarding appropriate measures for validating the results of any advanced search methodologies applied to identify potentially responsive ESI (e.g., analytics, predictive coding, technology-assisted review), including statistical sampling of the null set.

#### **IV. PRODUCTION FORMAT**

**A. Images.** Unless otherwise specified herein, all documents and ESI shall be produced as single-page, black and white Group IV Tagged Image File Format (TIFF) files of 300 DPI resolution, with corresponding multipage text and necessary load files (as discussed below). Page size shall be 8.5x11 inches unless, in the good faith judgment of the producing party, a particular item requires a different page size. Any documents that exist in hard copy at the time of their collection shall be scanned and produced electronically in the same format as TIFF format, and shall include multipage, document-level OCR text files with Unicode compliant (UTF-8) text that maximizes text quality. Settings such as “auto-skewing” and “auto-rotation” should be turned on during the OCR process. Original document orientation shall be maintained (i.e., portrait to portrait, and landscape to landscape). If an original document contains color, the document shall be produced as single-page, 300 DPI JPG images with JPG compression and a high quality setting as to not degrade the original image. Each TIFF/JPG image of an electronic document will be created directly from the corresponding native file, and all TIFFs/JPGs shall show any and all text and images that would be visible to the reader using the native software that created the document (e.g., for emails, the BCC line). The parties are under no obligation to enhance an image beyond how it was kept in the usual course of business. If the image does not accurately reflect the document as it was kept in the usual course of business, including all comments, edits, tracking, etc., the parties agree to meet and confer in good faith on production format options.

**B. Load File.** Each file shall be accompanied by an image load file, in standard .opt image cross-reference file format, showing the Bates number of each page, the appropriate unitization of the documents (*i.e.*, distinct documents shall not be merged into a single record, and single documents shall not be split into multiple records), and the entire family range.

**C. Text File.** Each ESI file produced shall be accompanied by a delimited multipage searchable database text file (*i.e.*, .dat) containing the delimited fields identified in Exhibit A, but no party will have any obligation to manually generate information for the fields identified in Exhibit A. Any files scanned from hard-copy documents shall include the following fields in the .dat text file: “BegDoc,” “EndDoc,” “PageCount,” “Text Path,” and “Custodian.” The text file shall contain full text extraction and be created by extracting text directly from the underlying native file unless the ESI must be redacted prior to production, in which case, the text file shall be generated by applying industry standard OCR technology to the reacted version of the ESI. Each text file shall be named with the beginning Bates number of the electronic file to which the text file relates.

**D. Bates Numbering.** All ESI and hard-copy documents that a party produces in TIFF or JPG format shall be electronically branded with a legible, unique Bates number on each page, but the Bates number should not be included in the extracted text of ESI. The Bates number shall: (1) identify the producing party; (2) maintain a constant length of eight numeric digits (including 0-padding) across the entire production; (3) contain only alphanumeric characters and dashes, no special characters or embedded spaces; and (4) be sequential within a given document. If the Bates number conceals, interferes with, or otherwise obscures any information from the source document, the Producing Party, at the request of the Receiving Party, shall produce a copy that is not so obscured. Each TIFF/JPG file shall be named with the same page-level Bates number



branded on the underlying image.

**E. Confidentiality Legend.** For ESI produced subject to a claim of confidentiality under the parties' proposed discovery confidentiality order (or any alternative confidentiality order entered in this case), the producing party shall electronically brand the appropriate confidentiality designation onto each page of the document, but should not include the confidentiality designation in the extracted text of the ESI. If the designation conceals, interferes with, or otherwise obscures any information from the source document, the Producing Party, at the request of the Receiving Party, shall produce a copy that is not so obscured.

**F. Naming Conventions.** TIFF or JPG image files shall be named according to the Bates number branded on the image (e.g., ABC-00000004.jpg). For documents produced in native file format, no Bates numbering or confidentiality legend should be added to the content of the document. Instead, native files shall be named according to the Bates number identified on the document's placeholder TIFF image (e.g., ABC-00000007.xlsx).

**G. Preservation of Families.** Parent-child relationships between electronic files (e.g., the association between an attachment and its parent email, or a spreadsheet embedded within a word processing document) must be preserved by producing attachments sequentially after the parent document, assigning sequential Bates numbers to all files within a parent-child group, and by providing accurate attachment ranges for those files in the metadata fields identified below. The parties further agree that if any part of a document family is responsive, the entire document family will be produced, except any to the extent the parent or child is subject to a valid claim of attorney client privilege or work product (discussed below). Electronic document families shall be produced in a manner that maintains the parent-child relationship that have been maintained in the ordinary course of business, with attachments produced sequentially after the parent email.

**H. Embedded Objects.** If a document has another file embedded in it, the Producing Party shall produce the document embedded file as an attachment to the document in which it is contained, with the parent-child relationship preserved, subject to the procedures below:

a. If the document is a PowerPoint file, the Producing Party need not extract the embedded files into independent stand-alone files. The Receiving Party may request in writing that the embedded document be produced as an extracted stand-alone file if it in good faith believes that the embedded file contains relevant and proportional information not found elsewhere.

b. If the document is a Word or Excel file, the Producing Party shall extract the embedded files into independent stand-alone files, which shall be searched consistent with the Producing Party's search methodology for other ESI.

c. If the embedded file is a logo, it need not be extracted as a separate document as long as they are displayed in the parent document.

d. If the document is any other file type, the Parties agree to meet and confer regarding extraction and production formats.

e. All embedded files produced as extracted documents under this procedure shall be subject to the same production requirements set forth herein, and in the load file shall refer to the parent document in which the file was embedded, and be marked with a "Yes" under the "Is Embedded" metadata field.

**I. Embedded Links.** The parties shall use their best efforts to collect and produce documents that are links in emails, including, but not limited to, Google G Suite, Microsoft O365, etc. Documents extracted from links shall be populated with the BEGATTACH and ENDATTACH metadata fields to show the family relationship.

**J. Compressed Files.** Compressed file types (e.g., .ZIP, .RAR, .CAB, .Z) should be decompressed so that the lowest level document or file is extracted.

**K. Dynamic Fields.** Unless otherwise agreed, all dynamic date and time fields, where such fields are processed to contain a value, and all metadata pertaining to dates and times, will be standardized to Universal Coordinated Time (UTC). The Parties understand and acknowledge that such standardization affects only dynamic fields and metadata values, and does not affect, among other things, dates and times that are hard-coded text within a file (e.g., in an email thread, dates and times of earlier messages that were converted to body text when subsequently replied to or forwarded; and, in any file type, dates and times that are typed as such by users). Dates and times that are hard-coded within a file will be produced as part of the document text.

**L. Hidden Content and Tracked Changes.** To the extent that a document contains hidden content, tracked changes, comments, notes, or other similar information, it shall be imaged so that such information is captured on the produced image file, in color and to the extent practicable, identifying various commenters, as applicable.

**M. Exception Report.** The producing party shall compile an exception report enumerating any unprocessed or unprocessable documents, their file type, and the file location.

**N. Metadata.** All ESI will be produced with a delimited, database load file that contains the metadata fields listed in Table 1, attached hereto. The metadata produced should have the correct encoding to enable preservation of the documents' original language. For ESI other than email and e-docs that do not conform to the metadata listed in Exhibit A, such as text messages, chat conversations, Instant Bloomberg, iMessage, Google Chat, Yammer, Slack or other collaboration tools, etc., the parties will meet and confer as to the appropriate metadata fields to be produced.

## V. EXCEPTIONS TO PRODUCTION FORMAT

**A. Encrypted Data.** If any data source or file is corrupted, password-protected, encrypted, or not readable by the Producing Party, the Producing Party shall make all efforts to access the data source or file and produce the responsive ESI and any additional information necessary to access it. In the event the Producing Party is unable to access the data source or file, the Parties agree to meet and confer with regard to the protocol undertaken and potential further actions, if any.

**B. Natives.** The following ESI shall be produced in native format: (i) Microsoft Excel and other spreadsheet files (including .csv and similar files); (ii) slide presentation files such as Microsoft PowerPoint—except to the extent such presentation files require redactions; (iii) Microsoft Access files; (iv) audio and video files such as .wav or .mpeg files; and (iv) ESI where the TIFF or JPG version is not reasonably usable. When producing ESI in native format, a single-page TIFF slip sheet stating “Document Produced in Native Format” shall be provided, and branded with a Bates number and any applicable confidentiality designation meeting the requirements herein. Each native file shall be named according to the Bates number it has been assigned and shall be linked directly to its corresponding record in the load file using the NATIVELINK field. The text and metadata for the underlying electronic file, including the original file name, shall also be provided per the procedures set forth herein. To the extent a party believes that specific documents or classes of documents not already identified in this protocol should be produced in native format, following the production of such documents in imaged format, it may request the producing party produce in native format any imaged files that: (i) are unreadable or illegible; (ii) are cut-off or missing data or information; (iii) cannot be utilized at a deposition or authenticated and/or entered at trial in their imaged format; (iv) contain track changes which the receiving party specifically requests be produced in native on the grounds that the author,

date and/or time of line edits are unreadable in imaged format; and (v) the receiving party reasonably believes should be produced in native format, which reasons it shall articulate. The producing party shall produce any native files requested based on (i)-(iii) above without objection and, with respect to requests premised on (iv)-(v), the producing party shall either produce the native file(s) requested or respond in writing with an explanation for why it will not produce such files.

**C. Messaging and Collaboration Tools.** The parties will meet and confer regarding the production format for text messages, chat conversations and data from ephemeral messaging systems, collaboration tools, mobile device applications, social media, and other cloud sources.

**D. Structured Data.** To the extent a response to discovery requires the production of electronic information stored in a database, the parties will meet and confer regarding methods of production. The parties will consider whether all relevant information may be provided by querying the database for discoverable information and generating a report in a reasonably usable and exportable electronic file.

**E. Other ESI.** If a party identifies responsive documents or information in a form that cannot reasonably be imaged, the parties shall meet and confer regarding the appropriate means for producing such documents or information.

## **VI. PRODUCTION AND DELIVERY**

**Production Media.** The Parties may deliver productions on digital media (such as a CD-ROM, DVD, or external hard drive) or via a secure internet transfer tool (such as SFTP or ShareFile). The Parties agree that productions are delivered when they are made available for download or when they are physically delivered on digital media. Each production shall be labeled with the production date, the Bates range, and a volume number, if appropriate.

**Security.** To maximize the security of information in transit, any media on which

documents are produced may be encrypted. In such cases, the producing party shall transmit the encryption key or password to the receiving party, under separate cover, contemporaneously with sending the encrypted media.

## **VII. PRIVILEGE AND REDACTION**

**A. Privileged Families.** A party must have a valid claim of attorney client privilege or work product as to each document withheld. Where a document being withheld pursuant to a claim of privilege or work product is a member of a document family, the producing party may withhold only the document that contains the privileged information and may not withhold any family member document unless it, too, is subject to a valid claim of privilege. To the extent that a document family contains a combination of privileged and non-privileged documents, and the parent document is privileged, a copy of the privileged parent document showing only the sender and recipient information and date shall be produced, with the remainder of the document redacted. To the extent that a document family contains a combination of privileged and non-privileged documents, and an attachment is privileged, the privileged attachments will be represented in the production with a placeholder TIFF image endorsed with a sequential Bates number that bears the legend “Document Withheld as Privileged.” For all documents that contain a responsive, non-privileged attachment, the following fields will be produced (if available) as part of the metadata load file to indicate the family relationship: BegDoc, EndDoc, BegAttach, EndAttach, and ParentID.

**B. Privilege Logs.** Within 21 days of substantially completing document production, the producing party shall produce a privilege log containing a list of all responsive documents being withheld pursuant to a valid claim of privilege or work product. Any privilege log produced by a party must, in all respects, comply with the Federal Rules of Civil Procedure. In addition, but not in substitution of any duties required under the Federal Rules of Civil Procedure:

1. All privilege logs shall include: (i) date of the document; (ii) document identifier; (iii) the name of the document's author or creator; (iv) the name(s) of all recipients (for emails, separately listing all direct recipients, all individuals CC'd, and individuals BCC'd); (for word-processing documents, all persons who edited the document; and for collaborative or shared-access documents, all persons who accessed the document); (v) the subject matter of the document withheld; and the basis of the privilege claimed.

2. At the time it produces a privilege log, the producing party shall also provide a list of the attorneys (whether internal or outside counsel) whose names appear on the log.

3. Identical duplicates of a document (based on MD5 or SHA-1 algorithms) need not be logged. Documents are not "identical" for these purposes when the recipients of the documents are different.

4. A party need not log on a privilege log: (i) communications exclusively between a party or its representative(s) and its counsel after the commencement of litigation, and which relate to this Action; and/or (ii) work product created by counsel, an agent of counsel, or a party at the direction of counsel after February 27, 2020 and which relate to this Action.

5. After receiving a privilege log, a receiving party may identify in writing any particular logged document or redaction that it believes requires further explanation and state the need for such information. The parties shall then meet and confer in good faith to try to reach a mutually agreeable solution. If the parties do not resolve their dispute, they may request resolution from the Court.

**C. Redactions.** A party may redact information subject to a valid claim of privilege or attorney work product. Redactions of responsive documents for relevance are presumptively impermissible. However, if a party believes in good faith that an otherwise responsive document contains information that is not relevant and that redaction of such information is necessary to protect certain personally sensitive or proprietary interests that are not sufficiently addressed through the parties' proposed discovery confidentiality order (or any alternative confidentiality order entered in this case), the producing party shall identify such documents and categories of information it proposes to redact, and the parties agree to meet and confer on a mechanism for producing such documents, including the scope and format of any such redactions. To the extent that any document contains information that has been redacted for privilege, it shall be produced in the form of a redacted TIFF image. Documents redacted for privilege shall be logged in the manner set forth above. If documents that the parties have agreed to produce in native format need to be redacted, the parties shall use native redaction tools, to the extent reasonably practicable, to apply such redactions. To the extent native redaction tools are not reasonably practicable, the producing party shall produce TIFF images with burned in redactions and a TIFF placeholder image, provided the TIFF images are reasonably usable. If redacting TIFF images, the producing party should make reasonable efforts to cause such images to legibly present all information in the spreadsheet. To the extent a document is produced with redactions, the producing party will populate a metadata field indicating as much.



Date: November 1, 2022

By: s/ Matthew A. Sklar

**WINSTON & STRAWN LLP**

James P. Smith III (admitted *pro hac vice*)  
Matthew L. DiRisio (admitted *pro hac vice*)  
200 Park Avenue  
New York, New York 10166  
Telephone: (212) 294-6700  
Facsimile: (212) 294-4700  
jpsmith@winston.com  
mdirisio@winston.com

**MCCARTER & ENGLISH, LLP**

Matthew A. Sklar  
Omar A. Barentto  
Four Gateway Center  
100 Mulberry St.  
Newark, NJ 07102  
Telephone: (973) 622-4444  
Facsimile: (973) 624-7070  
msklar@mccarter.com  
obarentto@mccarter.com

*Attorneys for Defendants*

Date: November 1, 2022

By: s/ Sharan Nirmul

**KESSLER TOPAZ**

**MELTZER & CHECK, LLP**

Sharan Nirmul  
David A. Bocian  
Joshua E. D'Ancona  
Vanessa M. Milan (admitted *pro hac vice*)  
Nathaniel C. Simon (admitted *pro hac vice*)  
280 King of Prussia Road  
Radnor, PA 19087  
Telephone: (610) 667-7706  
Facsimile: (610) 667-7056  
snirmul@ktmc.com  
dbocian@ktmc.com  
jdancona@ktmc.com  
vmilan@ktmc.com  
nsimon@ktmc.com

*Lead Counsel for Lead Plaintiff  
and the Putative Class*

**CARELLA, BYRNE, CECCHI, OLSTEIN,  
BRODY & AGNELLO P.C.**

James E. Cecchi  
Donald A. Ecklund  
5 Becker Farm Road  
Roseland, NJ 07068  
Telephone: (973) 994-1700  
Facsimile: (973) 994-1744  
jcecchi@carellabyrne.com  
decklund@carellabyrne.com

*Liaison Counsel for the Putative Class*

IT IS SO ORDERED.

Dated: November 2, 2022

s/ Cathy L. Waldor  
Hon. Cathy L. Waldor, U.S.M.J.